



BlackBerry UEM pour les sites sombres

Installation et Administration Guide

12.17

Table des matières

À propos de BlackBerry UEM pour les sites sombres.....	4
Fonctionnalités BlackBerry UEM prises en charge.....	4
Fonctionnalités BlackBerry UEM non prises en charge.....	4
Architecture : BlackBerry UEM pour les sites sombres.....	6
Installation ou mise à niveau de BlackBerry UEM dans un environnement de site sombre.....	8
Installer ou mettre à niveau BlackBerry UEM.....	8
Connexion à BlackBerry UEM.....	8
Première connexion à BlackBerry UEM.....	9
Configurer BlackBerry UEM pour les sites sombres.....	10
Ajout de licences à BlackBerry UEM.....	11
Importer des licences BlackBerry UEM.....	11
Définir des clés de licence Samsung Knox.....	12
Obtention d'un certificat APNs pour gérer les terminaux iOS.....	12
Obtenir un fichier CSR signé auprès de BlackBerry.....	12
Demander un certificat APNs auprès d'Apple.....	13
Enregistrer le certificat APNs.....	13
Gestion des utilisateurs et des terminaux dans un environnement de site sombre.....	14
Activation des terminaux.....	14
Types d'activation pris en charge.....	14
Préparer les utilisateurs à activer des terminaux.....	17
Activation des terminaux BlackBerry 10.....	20
Activation des terminaux Samsung Knox.....	24
Activation des terminaux iOS.....	29
Gestion des terminaux BlackBerry 10.....	31
Gestion des terminaux Samsung Knox.....	31
Configurer le VPN à l'aide de KNOX StrongSwan.....	32
Gestion des terminaux iOS.....	32
Documentation produit.....	34
Informations juridiques.....	35

À propos de BlackBerry UEM pour les sites sombres

BlackBerry UEM est une solution EMM multiplateforme de BlackBerry qui fournit une gestion complète des terminaux, des applications et du contenu, en offrant une sécurité et une connectivité intégrées.

Dans les environnements dotés des exigences les plus élevées en matière de sécurité, la connexion à des sites extérieurs comme le BlackBerry Infrastructure peut être limitée ou impossible. BlackBerry UEM pour les sites sombres a été conçu pour fournir une solution de gestion des terminaux mobiles sécurisée sans que BlackBerry UEM doive se connecter à BlackBerry Infrastructure et à d'autres services sur Internet.

Fonctionnalités BlackBerry UEM prises en charge

Les fonctionnalités BlackBerry UEM suivantes sont prises en charge dans un environnement de site sombre.

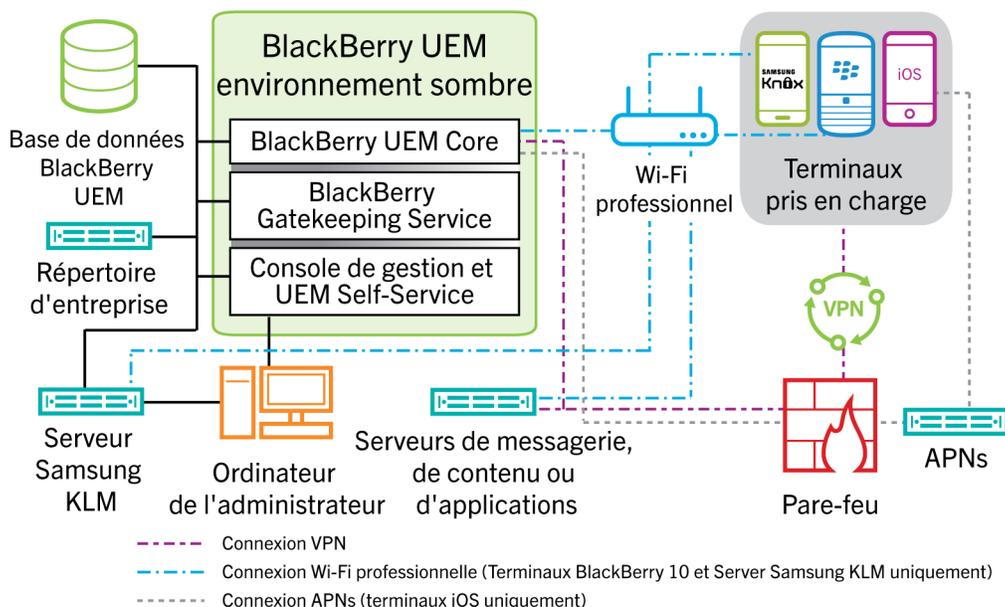
Fonctionnalité	Description
Gestion de terminaux multiplateforme	Vous pouvez gérer des terminaux BlackBerry 10, iOS et Samsung Knox.
Expérience approuvée et sécurisée	Les commandes des terminaux vous permettent de gérer avec précision la façon dont les terminaux se connectent à votre réseau, ainsi que de choisir les fonctionnalités à activer et les applications disponibles.
Contrôle de l'accès à Microsoft Exchange	Votre organisation peut utiliser BlackBerry Gatekeeping Service pour contrôler quels terminaux peuvent accéder à Exchange ActiveSync. Tout terminal ne figurant pas sur la liste blanche pour Microsoft Exchange est signalé dans la liste Terminals Exchange ActiveSync limités UEM et ne peut pas accéder aux données de l'organisateur et de la messagerie professionnelle.
Gestion des applications	Vous pouvez utiliser et gérer des applications internes sur les terminaux. Vous pouvez également empêcher les terminaux d'installer des applications d'autres sources.
Administration basée sur des rôles	Vous pouvez partager les tâches administratives avec plusieurs administrateurs qui peuvent accéder simultanément aux consoles d'administration. Vous pouvez utiliser des rôles pour définir les opérations qu'un administrateur peut effectuer et réduire les risques de sécurité, répartir les responsabilités des différents postes et augmenter l'efficacité en limitant les options disponibles pour chaque administrateur. Vous pouvez utiliser des rôles prédéfinis ou créer vos propres rôles personnalisés.

Fonctionnalités BlackBerry UEM non prises en charge

Les fonctionnalités BlackBerry UEM suivantes ne sont pas prises en charge dans un environnement de site sombre. Ces fonctionnalités sont désactivées dans BlackBerry UEM pour les sites sombres.

Fonctionnalités non prises en charge	Explication
Terminaux	BlackBerry UEM pour les sites sombres prend uniquement en charge les terminaux BlackBerry 10, iOS et Samsung.
Connectivité d'entreprise	<p>Les fonctionnalités BlackBerry UEM qui autorisent les terminaux à se connecter aux ressources de votre entreprise par le biais de BlackBerry Infrastructure ne sont pas prises en charge, y compris :</p> <ul style="list-style-type: none"> • BlackBerry Secure Connect Plus • BlackBerry Secure Gateway • BlackBerry MDS Connection Service • Utilisation de BlackBerry UEM comme proxy pour les demandes SCEP
BlackBerry Dynamics	Les applications BlackBerry Dynamics, y compris BlackBerry Work, ne sont pas prises en charge.
Autres produits d'entreprise BlackBerry	<p>BlackBerry UEM pour les sites sombres ne fonctionne pas avec d'autres produits d'entreprise BlackBerry, y compris :</p> <ul style="list-style-type: none"> • BlackBerry Enterprise Identity • BlackBerry 2FA
Gestion d'applications publiques et d'applications protégées par Microsoft Intune	<p>BlackBerry UEM pour les sites sombres ne prend pas en charge les connexions aux fournisseurs d'applications publiques, comme BlackBerry World, Apple App Store et Google Play. Vous ne pouvez pas ajouter d'applications publiques aux terminaux des utilisateurs.</p> <p>BlackBerry UEM pour les sites sombres ne prend pas en charge les connexions à Microsoft Azure. Vous ne pouvez pas gérer des applications à l'aide de profils de protection d'applications Microsoft Intune.</p>

Architecture : BlackBerry UEM pour les sites sombres



Nom du composant	Description
BlackBerry UEM Core	<p>BlackBerry UEM Core est le composant central de l'architecture BlackBerry UEM. Il consiste en de nombreux sous-composants responsables des fonctions suivantes :</p> <ul style="list-style-type: none"> Fonctions de journalisation, de surveillance, de génération de rapports et de gestion Services d'authentification et d'autorisation Planification et envoi de commandes, de stratégies informatiques et de profils aux terminaux
Base de données BlackBerry UEM	<p>La base de données BlackBerry UEM est une base de données relationnelle qui contient les informations des comptes d'utilisateurs et les informations de configuration utilisées par BlackBerry UEM pour gérer les terminaux.</p>
BlackBerry Gatekeeping Service	<p>BlackBerry Gatekeeping Service envoie les commandes à Exchange ActiveSync pour ajouter les terminaux à une liste autorisée lorsque ceux-ci sont activés sur BlackBerry UEM. Les terminaux non gérés qui tentent de se connecter au serveur de messagerie d'une entreprise peuvent être examinés, vérifiés et bloqués ou autorisés par un administrateur via la console de gestion de BlackBerry UEM.</p>

Nom du composant	Description
Console de gestion et UEM Self-Service	<p>La console de gestion et UEM Self-Service fournissent une interface utilisateur basée sur navigateur pour l'accès administrateur et utilisateur à BlackBerry UEM.</p> <p>La console de gestion vous permet de gérer les paramètres système, les utilisateurs, les terminaux et les applications.</p> <p>Les utilisateurs peuvent utiliser UEM Self-Service pour définir un mot de passe d'activation et envoyer des commandes aux terminaux, par exemple pour définir un mot de passe, verrouiller le terminal et supprimer les données de leurs terminaux.</p>
Serveurs de messagerie, de contenu ou d'applications	<p>Votre réseau interne comprend divers services avec lesquels les périphériques et BlackBerry UEM peuvent communiquer.</p> <p>Si vous activez des terminaux Samsung Knox à l'aide des types d'activation Android Enterprise, vous avez besoin d'un serveur contenant le fichier .apk BlackBerry UEM Client et d'un fichier PAC qui empêche les terminaux de tenter de se connecter à Google Play pendant l'activation.</p>
Serveur KLM Samsung	<p>Si vous gérez des terminaux Samsung Knox, un serveur de gestion des licences Samsung Knox est installé avec BlackBerry UEM pour les sites sombres afin que BlackBerry UEM n'ait pas besoin de se connecter au système de gestion des licences Samsung Knox basé sur le Web pour obtenir les informations de licence.</p> <p>Les terminaux Samsung Knox communiquent avec le serveur KLM à l'aide de votre réseau Wi-Fi professionnel.</p>
APNs	<p>Pour gérer les terminaux iOS, BlackBerry UEM doit envoyer des notifications aux terminaux par l'intermédiaire d'un serveur d'APNs. Lorsque les terminaux reçoivent une notification depuis des APNs, ils contactent BlackBerry UEM pour rechercher des mises à jour.</p> <p>Pour en savoir plus sur la sécurisation des connexions aux APNs ou sur de possibles alternatives à l'utilisation d'APNs publics, contactez votre responsable technique Apple.</p>

Installation ou mise à niveau de BlackBerry UEM dans un environnement de site sombre

Seuls les composants suivants sont activés pour BlackBerry UEM installé dans un environnement de site sombre :

- Console de gestion de BlackBerry UEM
- BlackBerry UEM Core
- BlackBerry Gatekeeping Service

Vous pouvez mettre à niveau BlackBerry UEM. Pour plus d'informations sur la migration des terminaux vers un nouvel environnement BlackBerry UEM, [reportez-vous au contenu relatif à la configuration de BlackBerry UEM](#).

Lorsque vous installez ou mettez à niveau BlackBerry UEM, vous pouvez utiliser un Microsoft SQL Server existant ou installer et utiliser Microsoft SQL Server Express.

Remarque : Avant d'installer ou de mettre à niveau BlackBerry UEM, consultez les exigences et les conditions préalables dans le [contenu relatif à la planification de BlackBerry UEM](#) et le [contenu relatif à l'installation et à la mise à niveau](#). Les exigences relatives aux ports se trouvent dans le [contenu relatif à la planification](#).

Installer ou mettre à niveau BlackBerry UEM

1. Connectez-vous en tant qu'utilisateur avec des privilèges d'administrateur local au serveur sur lequel vous installez ou mettez à niveau BlackBerry UEM.
2. Téléchargez et décompressez les fichiers d'installation BlackBerry UEM.
3. Modifiez le fichier `deployer.properties` avec les paramètres de votre environnement. Le fichier `deployer.properties` est situé dans le même dossier que le fichier `setup.exe`.
 - a) Dans le champ **service.compte.password** =, saisissez le mot de passe du compte sous lequel vous êtes connecté.
 - b) Si vous voulez utiliser un Microsoft SQL Server existant, saisissez les informations dans les champs appropriés pour ce serveur.

Pour plus d'informations sur la façon de remplir les différents champs, reportez-vous au [fichier `deployer.properties`](#) dans le contenu relatif à l'installation et à la mise à niveau de BlackBerry UEM.

4. Ouvrez une fenêtre d'invite de commande en tant qu'administrateur et, dans le répertoire où vous avez décompressé les fichiers d'installation BlackBerry UEM, saisissez l'une des commandes suivantes :

Option	Commande
Pour utiliser une base de données Microsoft SQL Server existante	<pre>setup.exe --script --iacceptbeseula --propertyFiles darksite.properties --showlog</pre>
Pour installer une base de données Microsoft SQL Server locale	<pre>setup.exe --script --iacceptbeseula --propertyFiles darksite.properties --showlog --installSQL</pre>

Connexion à BlackBerry UEM

Après avoir installé BlackBerry UEM, connectez-vous à la console de gestion.

Remarque : Lorsque vous vous connectez à BlackBerry UEM pour la première fois, en plus de fournir le nom de votre entreprise, l'identifiant et la clé d'authentification SRP, vous devez saisir le **nom du fichier de licence**. Vous obtenez le fichier de licence auprès de votre représentant commercial BlackBerry. L'identifiant et la clé d'authentification SRP doivent correspondre aux informations contenues dans le fichier de licence.



ATTENTION : Ne réutilisez pas les ID SRP d'anciennes instances de BES5, BES10, BES12 ou BlackBerry UEM lorsque vous installez une nouvelle instance de BlackBerry UEM.

Première connexion à BlackBerry UEM

Avant de commencer : Vérifiez que vous disposez de l'identifiant SRP BlackBerry UEM et de la clé d'authentification SRP.

Si l'application de configuration est toujours ouverte, vous pouvez accéder à la console de gestion directement depuis la boîte de dialogue Adresses de la console.

1. Dans le navigateur, saisissez **https://<server_name>:<port>/admin**, où <server_name> désigne le FQDN de l'ordinateur qui héberge la console de gestion. Le port par défaut de la console de gestion est le port 443.
2. Dans le champ **Nom d'utilisateur**, saisissez **admin**.
3. Dans le champ **Mot de passe**, saisissez **password**.
4. Cliquez sur **Connexion**.
5. Dans la liste déroulante Emplacement du serveur, sélectionnez le pays de l'ordinateur où BlackBerry UEM a été installé et cliquez sur **Suivant**.
6. Saisissez le nom de votre organisation, l'identifiant SRP et la clé d'authentification SRP.
7. Cliquez sur **Submit**.
8. Modifiez le mot de passe temporaire par un mot de passe permanent.
9. Cliquez sur **Submit**.

À la fin :

- Lorsque vous vous connectez à la console de gestion, vous pouvez choisir de suivre ou de fermer la boîte de dialogue **Bienvenue dans BlackBerry UEM**. Si vous fermez la boîte de dialogue, elle n'apparaîtra pas lors des tentatives de connexion suivantes.

Configurer BlackBerry UEM pour les sites sombres

Le tableau suivant résume les tâches de configuration que vous devez peut-être effectuer après avoir installé BlackBerry UEM dans un environnement de site sombre.

Pour plus d'informations sur la configuration de BlackBerry UEM, reportez-vous au [contenu relatif à la configuration de BlackBerry UEM](#).

Tâche	Description
Importer un fichier de licence BlackBerry UEM	<p>Vous devez importer manuellement les informations de licence dans BlackBerry UEM dans un environnement de site sombre.</p> <p>Pour plus d'informations, reportez-vous à Ajout de licences à BlackBerry UEM.</p>
Remplacer les certificats par défaut par des certificats approuvés	<p>Vous pouvez remplacer le certificat SSL par défaut utilisé par les consoles BlackBerry UEM et le certificat par défaut utilisé par BlackBerry UEM pour signer le profil MDM des terminaux iOS par des certificats approuvés.</p> <p>Pour plus d'informations, reportez-vous à la section Modification de certificats BlackBerry UEM dans le contenu relatif à la configuration de BlackBerry UEM.</p>
Configurer des connexions via des serveurs proxy internes	<p>Si votre entreprise utilise un serveur proxy pour établir la connexion entre les serveurs de votre réseau, vous devez peut-être configurer les paramètres proxy côté serveur pour permettre à BlackBerry UEM Core de communiquer avec les instances à distance de la console de gestion.</p> <p>Pour plus d'informations, reportez-vous à la section Configuration des connexions via des serveurs proxy internes dans le contenu relatif à la configuration de BlackBerry UEM.</p>
Connecter BlackBerry UEM à des répertoires d'entreprise	<p>Vous pouvez connecter BlackBerry UEM à un ou plusieurs répertoires d'entreprise pour que BlackBerry UEM puisse accéder aux données des utilisateurs et créer des comptes d'utilisateurs.</p> <p>Pour plus d'informations, reportez-vous à la section Connexion à vos répertoires d'entreprise dans le contenu relatif à la configuration de BlackBerry UEM.</p>
Connecter BlackBerry UEM à un serveur SMTP	<p>Si vous souhaitez que BlackBerry UEM envoie des e-mails d'activation et d'autres notifications aux utilisateurs, vous devez spécifier les paramètres de serveur SMTP que BlackBerry UEM peut utiliser.</p> <p>Pour plus d'informations, reportez-vous à la section Connexion à un serveur SMTP pour envoyer des notifications par e-mail dans le contenu relatif à la configuration de BlackBerry UEM.</p>

Tâche	Description
Obtenir et enregistrer un certificat APNs	<p>Si vous souhaitez gérer et envoyer des données aux terminaux iOS, vous devez vous procurer un fichier CSR signé auprès de BlackBerry, l'utiliser pour obtenir un certificat APNs auprès de Apple et enregistrer le certificat APNs auprès du domaine BlackBerry UEM.</p> <p>Pour plus d'informations, reportez-vous à Obtention d'un certificat APNs pour gérer les terminaux iOS.</p>
Désigner les terminaux autorisés à accéder à Exchange ActiveSync	<p>Si vous avez configuré Microsoft Exchange de manière à empêcher les terminaux d'accéder à la messagerie et aux données de l'organiseur professionnelles, à moins que les terminaux ne soient ajoutés à une liste autorisée, vous devez créer une configuration Microsoft Exchange dans BlackBerry UEM.</p> <p>Pour plus d'informations, reportez-vous à Contrôle des terminaux autorisés à accéder à Exchange ActiveSync dans le contenu relatif à l'administration de BlackBerry UEM.</p>
Configurer BlackBerry UEM Self-Service	<p>Si vous souhaitez autoriser les utilisateurs à effectuer certaines tâches de gestion (changer leur mot de passe, par exemple), vous pouvez configurer et distribuer l'application Web BlackBerry UEM Self-Service.</p> <p>Pour plus d'informations, reportez-vous à Configurer BlackBerry UEM Self-Service pour les utilisateurs dans le contenu relatif à l'administration de BlackBerry UEM.</p>

Ajout de licences à BlackBerry UEM

Lorsque BlackBerry UEM est installé dans un environnement de site sombre, vous devez importer manuellement les informations de licence dans BlackBerry UEM.

Si vous gérez des terminaux Samsung Knox, vous devez également définir des clés de licence ELM et KLM Samsung Knox.

Pour éviter de mettre à jour les licences manuellement à l'avenir, en particulier pour les terminaux Samsung Knox, songez à acheter des licences permanentes pour l'environnement de site sombre de votre organisation.

Vous pouvez obtenir un fichier de licence BlackBerry UEM et des clés de licence Samsung auprès de votre représentant commercial BlackBerry.

Importer des licences BlackBerry UEM

Avant de commencer : Obtenez un fichier de licence BlackBerry UEM auprès de votre représentant commercial BlackBerry.

1. Sur la barre de menus, cliquez sur **Paramètres > Licences**.
2. Sur la page **Résumé des licences**, cliquez sur **Importer la licence**.
Si vous souhaitez mettre à jour les licences existantes, cliquez plutôt sur **Mettre à jour les licences**.
3. Cliquez sur **Parcourir**.
4. Sélectionnez le fichier de licence à utiliser.
5. Cliquez sur **Ouvrir**.

Définir des clés de licence Samsung Knox

Si vous gérez des terminaux Samsung Knox dans un environnement de site sombre, vous devez définir des clés de licence Samsung Knox dans BlackBerry UEM.

Avant de commencer : Obtenez les clés de licence ELM et KLM Samsung Knox auprès de votre représentant commercial BlackBerry.

1. Sur la barre de menus, cliquez sur **Paramètres > Licences**.
2. Sur la page **Résumé des licences**, cliquez sur **Définir des clés de licence KNOX**.
3. Collez les clés de licence ELM Samsung Knox et KLM Samsung Knox dans les champs appropriés.
4. Cliquez sur **Enregistrer**.

Obtention d'un certificat APNs pour gérer les terminaux iOS

APNs (Apple Push Notification Service) est le service de notification Push d'Apple. Pour gérer les terminaux iOS, Apple exige que BlackBerry UEM puisse se connecter aux APNs. Pour en savoir plus sur la sécurisation des connexions aux APNs ou sur de possibles alternatives à l'utilisation d'APNs publics, contactez votre responsable technique Apple.

Vous devez vous procurer un certificat APNs pour utiliser BlackBerry UEM afin de gérer les terminaux iOS.

Remarque : Chaque certificat APNs est valable un an. La console d'administration affiche la date d'expiration. Vous devez renouveler le certificat APNs avant la date d'expiration en utilisant le même ID Apple que celui utilisé pour obtenir le certificat. Si le certificat expire, les terminaux ne reçoivent pas de données de BlackBerry UEM. Si vous enregistrez un nouveau certificat APNs, les utilisateurs doivent réactiver leurs terminaux pour recevoir des données.

Pour plus d'informations, [rendez-vous sur https://developer.apple.com](https://developer.apple.com) pour lire la section *Problèmes rencontrés lors de l'envoi de notifications Push* de l'article TN2265.

Il est recommandé d'accéder à la console d'administration et au portail de certificats Push Apple à l'aide des navigateurs Google Chrome ou Safari. Ces navigateurs offrent une prise en charge optimale pour la demande et l'enregistrement d'un certificat APNs.

Pour obtenir et enregistrer un certificat APNs afin d'utiliser les APNs publics, procédez comme suit :

Étape	Action
1	Obtenir un fichier CSR signé auprès de BlackBerry.
2	Utilisez le fichier CSR signé pour demander un certificat APNs à Apple.
3	Enregistrer le certificat APNs.

Obtenir un fichier CSR signé auprès de BlackBerry

Avant de pouvoir obtenir un certificat APNs, vous devez vous procurer un fichier CSR signé auprès de BlackBerry.

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Notification push Apple**.
2. Cliquez sur **Obtenir les certificats APNs**.

Si vous souhaitez renouveler le certificat APNs actuel, cliquez plutôt sur **Renouveler le certificat**.

3. Dans la section **Étape 1 sur 3 - Télécharger le certificat CSR signé auprès de BlackBerry**, cliquez sur **Télécharger la demande de signature de certificat**.
4. Cliquez sur **Enregistrer** pour enregistrer le fichier CSR non signé (.scsr) sur votre ordinateur.
5. Envoyez le fichier CSR non signé à votre BlackBerry représentant de l'assistance client.
Votre représentant de l'assistance client aura le fichier CSR signé par une AC BlackBerry et vous renverra le CSR signé.

À la fin : [Demander un certificat APNs auprès d'Apple](#).

Demander un certificat APNs auprès d'Apple

Avant de commencer : [Obtenir un fichier CSR signé auprès de BlackBerry](#).

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Notification push Apple**.
2. Dans la section **Étape 2 sur 3 - Obtenir un certificat APNs auprès d'Apple**, cliquez sur **Apple Push Certificate Portal**. Vous êtes dirigé vers le portail Apple Push Certificates Portal.
3. Connectez-vous au portail Apple Push Certificates Portal en utilisant un ID Apple valide.
4. Suivez les instructions pour charger le fichier CSR signé (.scsr).
5. Téléchargez et enregistrez le certificat APNs (.pem) sur votre ordinateur.

À la fin : [Enregistrer le certificat APNs](#).

Enregistrer le certificat APNs

Avant de commencer : [Demander un certificat APNs auprès d'Apple](#).

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Notification push Apple**.
2. Dans la section **Étape 3 sur 3 - Inscrire le certificat APNs**, cliquez sur **Parcourir**. Accédez au certificat APNs (.pem) et sélectionnez-le.
3. Cliquez sur **Submit**.

À la fin : Pour tester la connexion entre BlackBerry UEM et le serveur APNs, cliquez sur **Tester le certificat APNs**.

Gestion des utilisateurs et des terminaux dans un environnement de site sombre

Les tâches de gestion des utilisateurs et des terminaux pour la plupart des fonctionnalités prises en charge dans un environnement de site sombre sont les mêmes que dans n'importe quel autre environnement BlackBerry UEM. Pour obtenir des instructions sur la plupart des tâches administratives qui ne sont pas traitées dans le présent document, [reportez-vous au contenu relatif à l'administration de BlackBerry UEM](#).

Activation des terminaux

Lorsque vous activez un terminal, vous l'associez à BlackBerry UEM afin de pouvoir gérer le terminal et que les utilisateurs puissent accéder aux données professionnelles sur leur terminal.

Lorsqu'un terminal est activé, vous pouvez envoyer des stratégies informatiques et des profils pour contrôler les fonctionnalités disponibles et gérer la sécurité des données professionnelles. Vous pouvez également attribuer à l'utilisateur des applications à installer. Selon le niveau de contrôle lié au type d'activation sélectionné, vous pouvez également protéger le terminal en limitant l'accès à certaines données, en définissant à distance des mots de passe, en verrouillant le terminal ou en supprimant des données.

Types d'activation pris en charge

BlackBerry UEM pour les sites sombres prend en charge les types d'activation suivants pour les terminaux BlackBerry 10, Samsung Knox et iOS.

Terminals BlackBerry 10

Type d'activation	Description
Travail et Personnel - Entreprise	<p>Ce type d'activation fournit un contrôle des données professionnelles sur les terminaux, tout en veillant à assurer la confidentialité des données personnelles. Lorsqu'un terminal est activé, un espace Travail séparé est créé sur le terminal et l'utilisateur doit définir un mot de passe pour accéder à l'espace Travail. Les données professionnelles sont protégées à l'aide du cryptage et de l'authentification par mot de passe. Toutes les données professionnelles des précédentes activations sont supprimées.</p> <p>Vous pouvez contrôler l'espace Travail sur le terminal à l'aide de commandes et de stratégies informatiques, mais vous ne pouvez contrôler aucun aspect de l'espace Personnel sur le terminal.</p>
Espace Travail uniquement	<p>Ce type d'activation offre un contrôle complet sur le terminal et ne fournit pas d'espace séparé pour les données personnelles. Lorsqu'un terminal est activé, l'espace Personnel et toutes les données professionnelles des précédentes activations sont supprimés. Un espace Travail est installé et l'utilisateur doit créer un mot de passe pour accéder au terminal. Les données professionnelles sont protégées à l'aide du cryptage et de l'authentification par mot de passe.</p> <p>Vous pouvez contrôler le terminal à l'aide de commandes et de stratégies informatiques.</p>

Type d'activation	Description
Travail et Personnel - Régulé	<p>Ce type d'activation permet de contrôler à la fois les données professionnelles et personnelles. Lorsqu'un terminal est activé, un espace Travail séparé est créé sur le terminal et l'utilisateur doit définir un mot de passe pour accéder à l'espace Travail. Les données professionnelles sont protégées à l'aide du cryptage et de l'authentification par mot de passe. Toutes les données professionnelles des précédentes activations sont supprimées.</p> <p>Vous pouvez contrôler à la fois l'espace Travail et l'espace Personnel sur le terminal à l'aide de commandes et de stratégies informatiques.</p>

Terminaux Samsung Knox

Remarque : Les types d'activation Samsung Knox seront obsolètes dans une future version. Les terminaux qui prennent en charge Knox Platform for Enterprise peuvent être activés à l'aide des types d'activation Android Enterprise. Pour plus d'informations, rendez-vous sur le site Web <https://support.blackberry.com/community> pour consulter l'article 54614.

Type d'activation	Description
Espace Travail uniquement (terminal Android Enterprise entièrement géré)	<p>Ce type d'activation vous permet de gérer le terminal dans son ensemble à l'aide de commandes et de règles de stratégie informatique. Ce type d'activation requiert que l'utilisateur restaure les réglages d'usine du terminal avant de procéder à l'activation. Le processus d'activation installe un profil de travail et aucun profil personnel. L'utilisateur doit créer un mot de passe pour accéder au terminal. Toutes les données du terminal sont protégées à l'aide du cryptage et d'une méthode d'authentification de type mot de passe.</p> <p>Lors de l'activation, le terminal installe automatiquement BlackBerry UEM Client et lui accorde des autorisations d'administrateur. Les utilisateurs ne peuvent pas révoquer les autorisations d'administrateur ni désinstaller l'application.</p> <p>Après l'activation, les terminaux Espace Travail uniquement disposent uniquement d'un ensemble limité d'applications standard préinstallées, telles qu'Appareil photo, Téléphone et Paramètres, ainsi que les applications que vous avez vous-même attribuées avec une disposition requise. La liste des applications préinstallées conservées dépend du fournisseur du terminal et de la version du système d'exploitation.</p> <p>Pour ce type d'activation, vous devez réinitialiser le terminal aux paramètres d'usine par défaut avant de l'activer. Si BlackBerry UEM Client est supprimé ou si le profil professionnel est supprimé du terminal, il est automatiquement réinitialisé aux paramètres d'usine par défaut.</p>

Type d'activation	Description
Travail et Personnel - Contrôle total (terminal Android Enterprise entièrement géré avec un profil professionnel)	<p>Ce type d'activation vous permet de gérer le terminal dans son ensemble à l'aide de commandes et de règles de stratégie informatique. Ce type d'activation crée un profil professionnel sur le terminal qui sépare les données professionnelles des données personnelles. Les données de l'espace Travail sont protégées à l'aide du cryptage et d'une méthode d'authentification de type mot de passe, PIN, schéma ou empreinte digitale. Ce type d'activation prend en charge la journalisation de l'activité du terminal (SMS, MMS et appels téléphoniques) dans les fichiers journaux BlackBerry UEM.</p> <p>Après l'activation, les terminaux Travail et Personnel - Contrôle total ne disposent que d'un ensemble limité d'applications standard préinstallées, telles qu'Appareil photo, Téléphone et Paramètres, dans l'espace Personnel.</p> <p>Pour ce type d'activation, vous devez réinitialiser le terminal aux paramètres d'usine par défaut avant de l'activer. Si BlackBerry UEM Client est supprimé ou si le profil professionnel est supprimé du terminal, il est automatiquement réinitialisé aux paramètres d'usine par défaut.</p> <p>Lors de l'activation, les utilisateurs doivent octroyer les autorisations d'administrateur à BlackBerry UEM Client.</p>
Travail et Personnel - Confidentialité des données de l'utilisateur (Android Enterprise avec profil professionnel)	<p>Ce type d'activation préserve la confidentialité des données personnelles, mais vous permet de gérer les données professionnelles à l'aide de commandes et de règles de stratégie informatique. Ce type d'activation crée un profil professionnel sur le terminal qui sépare les données professionnelles des données personnelles. Les données professionnelles et personnelles sont protégées à l'aide du cryptage et de l'authentification par mot de passe.</p> <p>Les utilisateurs ne sont pas tenus d'octroyer des autorisations d'administrateur à BlackBerry UEM Client.</p>
Espace Travail uniquement - (Samsung Knox)	<p>Ce type d'activation vous permet de gérer le terminal dans son ensemble à l'aide de commandes et de règles de stratégie informatique Samsung Knox. Ce type d'activation supprime l'espace Personnel et installe un espace Travail. L'utilisateur doit créer un mot de passe pour accéder au terminal. Toutes les données du terminal sont protégées à l'aide du cryptage et d'une méthode d'authentification de type mot de passe, PIN, schéma ou empreinte digitale. Ce type d'activation prend en charge la journalisation de l'activité du terminal (SMS, MMS et appels téléphoniques) dans les fichiers journaux BlackBerry UEM.</p> <p>Lors de l'activation, les utilisateurs doivent octroyer les autorisations d'administrateur à BlackBerry UEM Client.</p>

Type d'activation	Description
Travail et Personnel - Contrôle total (Samsung Knox)	<p>Ce type d'activation vous permet de gérer le terminal dans son ensemble à l'aide de commandes et de règles de stratégie informatique Samsung Knox. Ce type d'activation crée un espace Travail séparé sur le terminal et l'utilisateur doit créer un mot de passe pour accéder à cet espace Travail. Les données de l'espace Travail sont protégées à l'aide du cryptage et d'une méthode d'authentification de type mot de passe, PIN, schéma ou empreinte digitale. Ce type d'activation prend en charge la journalisation de l'activité du terminal (SMS, MMS et appels téléphoniques) dans les fichiers journaux BlackBerry UEM.</p> <p>Lors de l'activation, les utilisateurs doivent octroyer les autorisations d'administrateur à BlackBerry UEM Client.</p>

Terminaux iOS

Type d'activation	Description
Contrôles MDM	<p>Ce type d'activation fournit une gestion de base des terminaux à l'aide des commandes de terminaux mises à disposition par iOS. Aucun espace Travail séparé n'est installé sur le terminal et aucune sécurité n'est ajoutée pour les données professionnelles. Vous pouvez contrôler le terminal à l'aide de commandes et de stratégies informatiques.</p>

Préparer les utilisateurs à activer des terminaux

Pour vous préparer à autoriser les utilisateurs à activer les terminaux, vous devez créer un profil d'activation, modifier le modèle d'e-mail d'activation et définir un mot de passe d'activation pour l'utilisateur.

Un profil d'activation indique le nombre et le type de terminaux qu'un utilisateur peut activer et le type d'activation à utiliser pour chaque type de terminal. Le profil d'activation attribué ne s'applique qu'aux terminaux activés par l'utilisateur après que vous avez attribué le profil. Les terminaux déjà activés ne sont pas automatiquement mis à jour pour correspondre au profil d'activation nouveau ou mis à jour.

Lorsque vous ajoutez un utilisateur à BlackBerry UEM, le profil d'activation par défaut est attribué au compte d'utilisateur. Par défaut, le profil d'activation permet l'activation des options qui ne sont pas prises en charge dans un environnement de site sombre. Vous pouvez modifier le profil d'activation par défaut selon vos besoins ou créer un profil d'activation personnalisé et l'attribuer aux utilisateurs ou groupes d'utilisateurs.

Le modèle d'e-mail d'activation définit l'e-mail envoyé aux utilisateurs leur demandant d'activer leur terminal.

Une fois le profil d'activation et le modèle d'e-mail terminés, vous pouvez définir un mot de passe d'activation pour l'utilisateur et envoyer un e-mail d'activation pour leur permettre de terminer l'activation.

Créer un profil d'activation

Remarque : Le profil d'activation affiche les options de terminal et de type d'activation qui ne sont pas prises en charge dans un environnement de site sombre. Lorsque vous créez ou mettez à jour un profil d'activation, ne sélectionnez pas d'options non prises en charge.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Stratégie > Activation**.
3. Cliquez sur **+**.

4. Saisissez le nom et la description du profil.
5. Dans le champ **Nombre de terminaux qu'un utilisateur peut activer**, spécifiez le nombre maximum de terminaux que l'utilisateur peut activer.
6. Dans la liste déroulante **Propriété du terminal**, effectuez l'une des actions suivantes :
 - Si certains utilisateurs activent des terminaux personnels et d'autres des terminaux professionnels, sélectionnez **Non spécifié**.
 - Sélectionnez **Travail** si la plupart des utilisateurs activent des terminaux professionnels.
 - Sélectionnez **Personnel** si la plupart des utilisateurs activent leurs terminaux personnels.
7. Vous pouvez, à votre convenance, sélectionner un avis d'entreprise dans la liste déroulante **Attribuer un avis d'entreprise**. Si vous affectez un avis d'entreprise, les utilisateurs activant des terminaux BlackBerry 10 ou iOS doivent accepter l'avis pour terminer le processus d'activation.
8. Dans la section **Types de terminaux que les utilisateurs peuvent activer**, sélectionnez les types de terminaux selon les besoins. Les types de terminaux que vous ne sélectionnez pas ne sont pas inclus dans le profil d'activation et les utilisateurs ne peuvent pas les activer.
9. Procédez comme suit pour chaque type de terminal inclus dans le profil d'activation :
 - a) Cliquez sur l'onglet correspondant au type de terminal.
 - b) Dans la liste déroulante **Restrictions relatives au modèle de terminal**, sélectionnez l'une des options suivantes :
 - **Aucune restriction** : les utilisateurs peuvent activer n'importe quel modèle de terminal.
 - **Autoriser les modèles de terminaux sélectionnés** : les utilisateurs peuvent activer uniquement les modèles de terminaux que vous spécifiez. Utilisez cette option pour limiter les terminaux autorisés à certains modèles uniquement.
 - **Ne pas autoriser les modèles de terminaux sélectionnés** : les utilisateurs ne peuvent pas activer les modèles de terminaux que vous spécifiez. Utilisez cette option pour bloquer l'activation de certains modèles ou terminaux de fabricants spécifiques.

Si vous limitez les modèles de terminaux que les utilisateurs peuvent activer, cliquez sur **Modifier** pour sélectionner les terminaux que vous souhaitez autoriser ou restreindre, puis cliquez sur **Enregistrer**.

- c) Dans la liste déroulante **Version minimale autorisée**, sélectionnez la version de système d'exploitation minimale autorisée.

De nombreuses versions de système d'exploitation antérieures ne sont plus prises en charge par BlackBerry UEM. Vous devez sélectionner une version minimale uniquement si vous ne souhaitez pas prendre en charge la version la plus ancienne actuellement prise en charge par BlackBerry UEM. Pour plus d'informations sur les versions prises en charge, [reportez-vous à la Matrice de compatibilité](#).

- d) Sélectionnez les types d'activation pris en charge.

Pour les terminaux Samsung Knox, vous pouvez sélectionner plusieurs types d'activation et les classer. Pour tous les autres types de terminaux, vous ne pouvez sélectionner qu'un seul type d'activation.

10. Pour les terminaux iOS, si vous souhaitez uniquement activer les terminaux supervisés, sélectionnez **Ne pas autoriser l'activation des terminaux non supervisés**.
11. Pour les terminaux Samsung, effectuez les actions suivantes :
 - a) Si vous avez sélectionné plusieurs types d'activation, cliquez sur les flèches vers le haut et vers le bas pour les classer.
 - b) Si vous avez sélectionné un type d'activation Android Enterprise, sélectionnez **Lors de l'activation de terminaux Android Enterprise, activez une fonctionnalité UEM Premium telle que BlackBerry Secure Connect Plus** pour activer les fonctionnalités de Knox Platform for Enterprise.
 - c) Décochez la case **Ajouter Google Play à l'espace Travail**.

Cette fonctionnalité n'est pas prise en charge dans un environnement de site sombre.

- d) Dans la section **Options d'attestation matérielle**, sélectionnez **Appliquer les règles de conformité d'attestation lors de l'activation** si vous souhaitez que BlackBerry UEM vérifie les terminaux lorsqu'ils sont activés pour s'assurer que le niveau de correctif de sécurité requis est installé.

12. Cliquez sur **Ajouter**.

Créer un modèle d'e-mail d'activation

1. Sur la barre de menus, cliquez sur **Paramètres > Paramètres généraux**.
 2. Cliquez sur **Modèles d'e-mail**.
 3. Cliquez sur **+**. Sélectionnez **Activation de terminal**.
 4. Dans le champ **Nom**, saisissez un nom pour identifier ce modèle.
 5. Dans le champ **Objet**, modifiez le texte pour personnaliser la ligne d'objet du premier e-mail d'activation.
 6. Dans le champ **Message**, saisissez le corps du texte de l'e-mail d'activation.
 - Utilisez l'éditeur HTML pour sélectionner le format de police et insérer des images (par exemple, un logo d'entreprise).
 - Insérez des variables dans le texte pour personnaliser le message (par exemple, utilisez la variable %UserDisplayName% pour insérer le nom du destinataire). Pour obtenir la liste des variables disponibles, reportez-vous [au contenu relatif à l'administration de BlackBerry UEM](#).
 - Pour les terminaux BlackBerry 10 et Samsung Knox, incluez l'adresse du serveur BlackBerry UEM dont les utilisateurs ont besoin pour activer le terminal.
 - Pour les terminaux BlackBerry 10, l'URL est : `http://nom.du.serveur:8882/SRP_ID/mdm`
 - Pour les terminaux Samsung Knox, l'URL est : `http://nom.du.serveur:8882/SRP_ID`
 - Pour obtenir un échantillon du texte, cliquez sur **Texte suggéré**.
 7. Pour envoyer le mot de passe d'activation et les instructions d'activation dans des e-mails distincts, sélectionnez **Envoyer deux e-mails d'activation distincts : le premier pour les instructions, le second pour le mot de passe**. Si vous décidez d'envoyer un seul e-mail d'activation, veillez à inclure le mot de passe d'activation (ou la variable correspondante) dans le premier e-mail.
 8. Dans le champ **Objet**, saisissez la ligne d'objet du second e-mail d'activation.
 9. Personnalisez le corps du texte du second e-mail d'activation que vous envoyez aux utilisateurs. Veillez à inclure le mot de passe d'activation ou la variable du mot de passe d'activation.
10. Cliquez sur **Enregistrer**.

Définir un mot de passe d'activation et envoyer un e-mail d'activation

Vous pouvez définir un mot de passe d'activation et envoyer à l'utilisateur un e-mail d'activation avec les informations nécessaires à l'activation d'un ou de plusieurs terminaux.

L'e-mail est envoyé depuis l'adresse électronique que vous avez configurée dans les paramètres de serveur SMTP.

Avant de commencer : [Créer un modèle d'e-mail d'activation](#).

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom du compte d'utilisateur.
4. Dans le volet Détails de l'activation, cliquez sur **Définir le mot de passe d'activation**.
5. Dans la liste déroulante **Option d'activation**, sélectionnez **Activation du terminal par défaut**.
6. Dans la liste déroulante **Mot de passe d'activation**, effectuez l'une des opérations suivantes :

- Si vous souhaitez que le mot de passe soit généré automatiquement, sélectionnez **Générer automatiquement le mot de passe d'activation du terminal et envoyer un e-mail contenant des instructions d'activation**. Lorsque vous sélectionnez cette option, vous devez choisir un modèle d'e-mail pour envoyer les informations à l'utilisateur.
 - Si vous souhaitez définir un mot de passe d'activation pour l'utilisateur et (facultatif) envoyer un e-mail d'activation, sélectionnez **Définir le mot de passe d'activation du terminal**.
7. Vous pouvez également modifier le champ Expiration de la période d'activation. Ce champ spécifie la durée de validité du mot de passe d'activation.
 8. Pour que le mot de passe d'activation ne s'applique qu'à une seule activation, sélectionnez **La période d'activation expire à l'issue de l'activation du premier terminal**.
 9. Dans la liste déroulante **Modèle d'e-mail d'activation**, sélectionnez le modèle d'e-mail que vous souhaitez utiliser.
 10. Cliquez sur **Submit**.

Activation des terminaux BlackBerry 10

Vous pouvez permettre aux utilisateurs d'activer des terminaux BlackBerry 10 par le biais de votre réseau Wi-Fi professionnel, ou vous pouvez activer plusieurs terminaux BlackBerry 10 pour les utilisateurs à l'aide de BlackBerry Wired Activation Tool.

Activation des terminaux BlackBerry 10 par le biais du Wi-Fi professionnel

Vous pouvez autoriser les utilisateurs à activer des terminaux BlackBerry 10 par le biais de votre réseau Wi-Fi professionnel. Pour activer des terminaux, les utilisateurs ont besoin des informations suivantes :

- Adresse électronique professionnelle
- Mot de passe d'activation
- Adresse du serveur BlackBerry UEM (http://server.name:8882/SRP_ID/mdm)

Vous pouvez fournir les informations dans l'e-mail d'activation que BlackBerry UEM envoie aux utilisateurs. Reportez-vous à la section [Créer un modèle d'e-mail d'activation](#).

Activer un terminal BlackBerry 10

Envoyez les instructions d'activation suivantes à l'utilisateur du terminal.

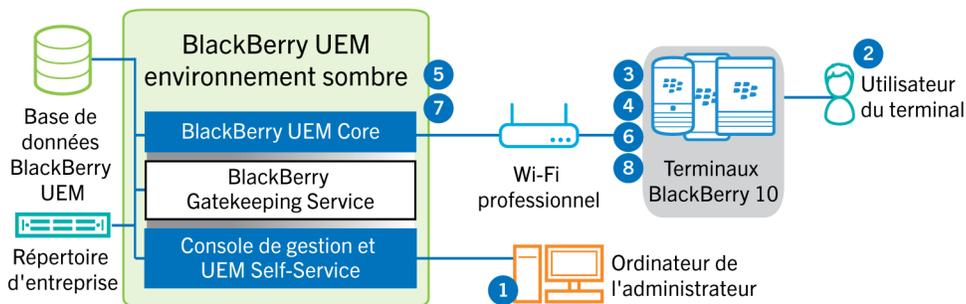
1. Sur le terminal, naviguez jusqu'à **Paramètres**.
2. Appuyez sur **Comptes**.
3. Si vous disposez de comptes existants sur ce terminal, appuyez sur **Ajouter un compte**. Sinon, passez à l'étape 4.
4. Appuyez sur **Messagerie, calendrier et contacts**.
5. Saisissez votre adresse électronique professionnelle et appuyez sur **Suivant**.
6. Dans le champ **Mot de passe**, saisissez le mot de passe d'activation que vous avez reçu. Appuyez sur **Suivant**. Vous recevrez un avertissement indiquant que votre appareil n'a pas pu chercher les informations de connexion.
7. Appuyez sur **Avancé**.
8. Appuyez sur **Compte professionnel**.
9. Dans le champ **Adresse du serveur**, saisissez l'adresse du serveur. Vous trouverez l'adresse du serveur dans l'e-mail d'activation que vous avez reçu ou dans BlackBerry UEM Self-Service.
10. Sélectionnez **Terminé**.

11. Suivez les instructions à l'écran pour terminer le processus d'activation.

À la fin : Pour vérifier que le processus d'activation a réussi, effectuez l'une des actions suivantes :

- Sur le terminal, accédez à BlackBerry Hub et vérifiez que l'adresse électronique est présente. Naviguez jusqu'au Calendrier et vérifiez que les rendez-vous sont présents.
- Dans BlackBerry UEM Self-Service, vérifiez que votre terminal est répertorié en tant que terminal activé. Le statut peut prendre jusqu'à deux minutes pour se mettre à jour après que vous avez activé le terminal.

Flux de données : activation d'un terminal BlackBerry 10



1. Vous effectuez les opérations suivantes :

- a. Ajoutez un utilisateur à BlackBerry UEM en tant que compte d'utilisateur local ou à l'aide des informations de compte récupérées depuis votre annuaire d'entreprise.
- b. Attribuer un profil d'activation à l'utilisateur
- c. Utilisez l'une des options suivantes pour fournir les détails d'activation à l'utilisateur :
 - Générez automatiquement un mot de passe d'activation du terminal et envoyez un e-mail contenant les instructions d'activation à l'utilisateur
 - Définissez un mot de passe d'activation du terminal et communiquez le nom d'utilisateur et le mot de passe à l'utilisateur directement ou par e-mail.
 - Communiquez l'adresse de BlackBerry UEM Self-Service à l'utilisateur afin qu'il puisse définir son propre mot de passe d'activation.

2. L'utilisateur effectue les opérations suivantes :

- a. Il se connecte à votre réseau Wi-Fi professionnel.
- b. Il saisit le nom d'utilisateur et le mot de passe d'activation sur le terminal
- c. Pour une activation « Travail et Personnel - Régulé » ou « Espace Travail uniquement », il accepte l'avis d'entreprise qui précise les conditions générales auxquelles l'utilisateur doit souscrire

3. Si l'activation est une activation « Espace Travail uniquement », le terminal supprime toutes les données existantes et redémarre.

4. Le terminal effectue les opérations suivantes :

- a. Il établit une connexion avec BlackBerry UEM.
- b. Il génère une clé symétrique partagée utilisée pour protéger le CSR et la réponse à BlackBerry UEM en utilisant le mot de passe d'activation ainsi que EC-SPEKE.
- c. Il crée un CSR et un HMAC cryptés comme suit :
 - Il génère une paire de clés pour le certificat
 - Il crée un CSR PKCS#10 qui inclut la clé publique de la paire de clés

- Il crypte le CSR à l'aide de la clé symétrique partagée et d'AES-256 en mode CBC avec remplissage PKCS#5
 - Il calcule un code HMAC du CSR crypté à l'aide de SHA-256 et l'ajoute au CSR
- d. Il envoie le CSR et le HMAC cryptés à BlackBerry UEM.
5. BlackBerry UEM effectue les actions suivantes :
- a. Il vérifie le HMAC du CSR crypté et décrypte le CSR à l'aide de la clé symétrique partagée
 - b. Il récupère le nom d'utilisateur, l'ID de l'espace Travail et le nom de votre organisation depuis la base de données BlackBerry UEM.
 - c. Il conditionne un certificat client à l'aide des informations récupérées et du CSR que le terminal a envoyé
 - d. Il signe le certificat client à l'aide du certificat racine de gestion d'entreprise
 - e. Il crypte le certificat client, le certificat racine de gestion d'entreprise et l'URL de BlackBerry UEM à l'aide de la clé symétrique partagée et d'AES-256 en mode CBC avec remplissage PKCS#5.
 - f. Il calcule un code HMAC du certificat client crypté, le certificat racine de gestion d'entreprise et l'URL de BlackBerry UEM et l'ajoute aux données cryptées.
 - g. Il envoie les données cryptées et le HMAC au terminal
6. Le terminal effectue les opérations suivantes :
- a. Il vérifie le HMAC
 - b. Il décrypte les données qu'il a reçues de BlackBerry UEM.
 - c. Il stocke le certificat client et le certificat racine de gestion d'entreprise dans sa base de stockage de clés
7. BlackBerry UEM effectue les actions suivantes :
- a. Il attribue le nouveau terminal à une instance BlackBerry UEM dans le domaine.
 - b. Il envoie les informations de configuration, notamment les paramètres de connectivité d'entreprise, au terminal
8. Le terminal envoie un message de confirmation via TLS à BlackBerry UEM pour confirmer qu'il a reçu et appliqué la stratégie informatique et les autres données et qu'il a créé l'espace Travail. Le processus d'activation est terminé.

Les protocoles de courbe elliptique utilisés pendant le processus d'activation utilisent la courbe à 521 bits recommandée par NIST.

Activation de terminaux BlackBerry 10 à l'aide de BlackBerry Wired Activation Tool

BlackBerry Wired Activation Tool vous permet d'activer simultanément plusieurs terminaux BlackBerry 10 dans un environnement sur site via des connexions USB au lieu de connexions sans fil. Votre entreprise peut être amenée à utiliser cette méthode pour différentes raisons :

- Pour accélérer et faciliter l'activation simultanée de plusieurs terminaux
- Pour continuer de confier le processus d'activation aux administrateurs
- Pour activer les terminaux et configurer leurs fonctions de sécurité, comme les exigences de cryptage de contenu et les profils VPN, avant de les confier aux utilisateurs ou de les connecter au réseau de votre organisation

Vous ne pouvez pas attribuer de profils ou de stratégies à l'aide de BlackBerry Wired Activation Tool. Vous devez attribuer les profils et les stratégies à vos utilisateurs dans la console de gestion BlackBerry UEM avant d'attribuer et d'activer les terminaux à l'aide de BlackBerry Wired Activation Tool. Il n'est cependant pas nécessaire de définir de mots de passe d'activation pour attribuer et activer des terminaux à l'aide de BlackBerry Wired Activation Tool.

Pour activer les terminaux à l'aide de BlackBerry Wired Activation Tool, les terminaux doivent exécuter BlackBerry 10 OS version 10.3 ou ultérieure.

BlackBerry Wired Activation Tool n'est pas pris en charge par BlackBerry UEM Cloud.

Pour obtenir le BlackBerry Wired Activation Tool, contactez votre représentant du service clientèle.

Configurer BlackBerry Wired Activation Tool et se connecter à une instance de BlackBerry UEM

Avant de pouvoir activer des terminaux avec BlackBerry Wired Activation Tool, vous devez créer une configuration pour chaque instance de BlackBerry UEM à laquelle vous devez accéder. Lorsque c'est chose faite, vous devez également utiliser un compte d'administrateur pour autoriser BlackBerry Wired Activation Tool à accéder à BlackBerry Web Services.

1. Dans le dossier d'installation de BlackBerry Wired Activation Tool, double-cliquez sur le fichier **BWAT.exe**.
2. Dans l'écran **Ajouter un serveur BES12**, dans le champ **Nom**, saisissez un nom pour identifier la configuration que vous créez. Par exemple, si vous disposez de deux instances BlackBerry UEM, vous pouvez créer une configuration pour chacune et les nommer Serveur 1 et Serveur 2.
3. Dans le champ **URL de BlackBerry Web Services**, saisissez l'adresse du composant BlackBerry Web Services. Par défaut, l'adresse est `https://<BlackBerry UEM web address>:18084`.

Pour changer de port, modifiez le paramètre `tomcat.bws.port` de la base de données BlackBerry UEM.

4. Dans le champ **URL du point de terminaison BCP**, saisissez l'adresse à utiliser pour les activations de terminaux. Ceci est également connu sous le terme d'URL d'activation ou de nom du serveur. Par défaut, l'adresse est : `http://server.name:8882/SRP_ID/mdm`.

Pour rechercher l'adresse, vérifiez que la variable `%ActivationURL%` se trouve dans le modèle d'e-mail d'activation et cliquez sur **Afficher l'e-mail d'activation** depuis un écran Synthèse des données utilisateur.

Si nécessaire, vous pouvez également rechercher le port et l'adresse de l'hôte dans la base de données BlackBerry UEM. Dans le tableau `def_cfg_setting_dfn`, recherchez les valeurs `id_setting_definition` pour `bdmi.enroll.bcp.host` et `bdmi.enroll.bcp.port`. Utilisez ensuite les valeurs `id_setting_definition` pour rechercher les valeurs de ces paramètres dans `obj_global_cfg_setting`.

5. Cliquez sur **Submit**.
6. Dans l'écran **Connexion**, sélectionnez une configuration BlackBerry UEM dans la liste déroulante.
7. Dans le champ **Nom d'utilisateur**, saisissez le nom d'utilisateur d'un compte d'utilisateur BlackBerry UEM doté d'autorisations d'administrateur.
8. Dans le champ **Mot de passe**, saisissez le mot de passe du compte.
9. Dans la liste déroulante **Répertoire**, sélectionnez une méthode d'authentification.
10. Si nécessaire, dans le champ **Domaine**, saisissez le domaine Microsoft Active Directory.
11. Cliquez sur **Se connecter**.

Activer des terminaux BlackBerry 10 à l'aide de BlackBerry Wired Activation Tool

Avant de commencer :

- Configurez BlackBerry Wired Activation Tool et connectez-vous à une instance de BlackBerry UEM.
 - Activez tous les terminaux connectés et vérifiez qu'ils ont terminé le processus de configuration initiale ou qu'ils ne l'ont pas démarré. Vous ne pouvez pas activer les terminaux si le processus de configuration initiale est en cours.
1. Connectez un ou plusieurs terminaux BlackBerry 10 à votre ordinateur à l'aide de câbles USB.
 2. Vérifiez la colonne **État** pour chaque terminal. Effectuez l'une des opérations suivantes :
 - Si la colonne État indique **Mot de passe requis**, cliquez sur **Mot de passe requis** pour saisir le mot de passe du terminal.
 - Si la colonne État indique **Terminal non pris en charge**, procédez à la mise à niveau de BlackBerry 10 OS vers la version 10.3 ou ultérieure.
 - Si la colonne État indique **Prêt**, attribuez le terminal à un utilisateur.

3. Dans le champ **Rechercher**, recherchez un compte d'utilisateur auquel vous souhaitez attribuer un terminal.
4. Dans la liste des résultats de la recherche, cliquez sur le compte d'utilisateur.
5. Dans la section principale de l'écran, cliquez sur le nom d'un compte d'utilisateur et faites-le glisser vers un terminal pour attribuer le terminal à cet utilisateur. Répétez cette étape pour attribuer des terminaux à plusieurs utilisateurs.
6. Cochez la case en regard des paires d'utilisateurs et de terminaux que vous souhaitez activer.
7. Cliquez sur **Activer les terminaux**.

BlackBerry Wired Activation Tool active tous les terminaux que vous avez sélectionnés. Vérifiez la colonne État pour connaître la progression et les résultats de chaque terminal. Si l'activation échoue, cliquez sur le message de la colonne État pour plus d'informations sur les erreurs.

Activation des terminaux Samsung Knox

Les utilisateurs peuvent activer des terminaux Samsung Knox par le biais de votre réseau Wi-Fi professionnel. BlackBerry UEM pour les sites sombres ne prend pas en charge « MDM Samsung Knox » ou les activations « Travail et Personnel - Confidentialité des données de l'utilisateur - (Samsung Knox) ». BlackBerry UEM pour les sites sombres ne prend également pas en charge Samsung Knox Mobile Enrollment.

Remarque : Les types d'activation Samsung Knox seront obsolètes dans une future version. Les terminaux qui prennent en charge Knox Platform for Enterprise peuvent être activés à l'aide des types d'activation Android Enterprise. Pour plus d'informations, rendez-vous sur le site Web <https://support.blackberry.com/community> pour consulter l'article 54614.

Pour activer un terminal, les utilisateurs ont besoin des informations suivantes :

- Adresse électronique professionnelle
- Mot de passe d'activation
- Adresse du serveur BlackBerry UEM (http://server.name:8882/SRP_ID)

Vous pouvez fournir les informations dans l'e-mail d'activation que BlackBerry UEM envoie aux utilisateurs. Reportez-vous à la section [Créer un modèle d'e-mail d'activation](#).

Si votre organisation utilise des terminaux Samsung Knox dans un environnement de site sombre, un serveur KLM Samsung a été installé avec BlackBerry UEM. Les terminaux Samsung Knox communiquent avec le serveur KLM à l'aide de votre réseau Wi-Fi professionnel. Si vous activez des terminaux avec des types d'activation Android Enterprise et que le certificat de serveur KLM est signé par une autorité de certification interne, vous devez envoyer le certificat de serveur KLM aux terminaux à l'aide d'un profil de certificat d'autorité de certification. Pour plus d'informations, reportez-vous au [contenu relatif à l'administration de BlackBerry UEM](#).

Étapes à suivre pour activer des terminaux Samsung Knox

Étape	Action
1	Créez les profils, applications et stratégies informatiques requis et attribuez-les aux utilisateurs. Si vous avez l'intention de configurer un VPN pour les terminaux Samsung Knox, Configurer le VPN à l'aide de KNOX StrongSwan .
2	Créer un profil d'activation et attribuez-le à un compte d'utilisateur ou à un groupe d'utilisateurs.
3	Définir un mot de passe d'activation et envoyer un e-mail d'activation.

Étape	Action
4	Fournissez des instructions d'activation aux utilisateurs pour les terminaux Android Enterprise ou Samsung KNOX Workspace .

Installation de BlackBerry UEM Client sur les terminaux Samsung Knox

Les utilisateurs doivent installer le BlackBerry UEM Client avant d'activer un terminal Samsung Knox. Vous pouvez télécharger manuellement le UEM Client à partir de BlackBerry et l'enregistrer dans un emplacement réseau auquel les appareils ont accès. Pour télécharger le fichier .apk du dernier UEM Client, rendez-vous sur le site [Web support.blackberry.com/community](http://support.blackberry.com/community) pour consulter l'article 42607.

Si les utilisateurs activent des terminaux à l'aide des types d'activation Samsung Knox Workspace ou Android Enterprise (Travail et Personnel - Confidentialité des données de l'utilisateur), vous pouvez leur demander d'obtenir et d'installer le UEM Client avant de commencer le processus d'activation.

Pour les terminaux qui seront activés avec les types d'activation Android Enterprise (Espace Travail uniquement) ou (Travail et Personnel - Contrôle total), le terminal doit être défini sur les paramètres d'usine par défaut avant de commencer l'activation. Vous pouvez définir des options d'activation pour installer le UEM Client à partir d'un serveur sur votre réseau pendant l'activation. Pour fournir l'emplacement de téléchargement au terminal, vous pouvez inclure l'emplacement dans un QR Code que l'utilisateur scanne pour lancer l'activation.

Définition des options d'activation pour les activations Android Enterprise

Pour les terminaux qui seront activés avec les types d'activation Android Enterprise (Espace Travail uniquement) ou (Travail et Personnel - Contrôle total), le terminal doit être défini sur les paramètres d'usine par défaut avant de commencer l'activation. Vous pouvez définir des options d'activation pour installer le BlackBerry UEM Client à partir d'un serveur sur votre réseau pendant l'activation. Pour fournir l'emplacement de téléchargement au terminal, vous pouvez inclure l'emplacement dans un QR Code que l'utilisateur scanne pour lancer l'activation.

Vous devez également créer un fichier PAC qui empêche les terminaux de tenter de se connecter à Google Play pendant l'activation et de stocker le fichier PAC au même emplacement que le fichier .apk UEM Client.

Avant de commencer : Téléchargez le UEM Client à partir de BlackBerry et enregistrez-le dans un emplacement réseau auquel les terminaux ont accès. Pour en savoir plus, rendez-vous sur support.blackberry.com/community pour consulter l'article 42607.

1. Créez un fichier PAC au format suivant qui spécifie l'URL HTTP où le fichier PAC est hébergé et enregistrez-le au même emplacement que le fichier .apk UEM Client.

```
function FindProxyForURL(url, host)
{
return "DIRECT";
}
```

Les utilisateurs devront spécifier l'**adresse Web PAC** lorsqu'ils auront configuré la connexion Wi-Fi sur leur terminal lors de l'activation. Le fichier PAC doit être disponible sur le port HTTP par défaut 80.

2. Dans la barre de menus, cliquez sur **Paramètres > Paramètres généraux**.
3. Cliquez sur **Paramètres d'activation par défaut**.
4. Sous **Paramètres d'activation de terminal par défaut**, définissez les options QR Code suivantes.
 - a) Sélectionnez **Autoriser les QR Codes pour l'activation des terminaux**.
 - b) Sélectionnez **Autoriser le QR Code à contenir l'emplacement du fichier source de l'application UEM Client**.

- c) Dans le champ **Emplacement du fichier source de l'application UEM Client**, spécifiez l'emplacement réseau où vous avez enregistré le fichier .apk.
5. Vérifiez que les options suivantes ne sont pas sélectionnées :
- **Activez le type d'activation Contrôles MDM pour les terminaux Android**
 - **Utiliser les QR Codes pour déverrouiller les applications BlackBerry Dynamics**
 - **Activer l'inscription auprès de BlackBerry Infrastructure**
6. Cliquez sur **Enregistrer**.

Activer un terminal Android Enterprise

Ces instructions s'appliquent aux types d'activation Android Enterprise (Espace Travail uniquement) ou (Travail et Personnel - Contrôle total). Ces terminaux doivent être définis sur les paramètres d'usine par défaut avant de commencer l'activation.

Pour les activations Android Enterprise (Travail et Personnel - Confidentialité des données de l'utilisateur), suivez les instructions pour [Activer un terminal Samsung Knox Workspace](#).

Envoyez les instructions d'activation suivantes à l'utilisateur du terminal.

1. Sur le terminal que vous souhaitez activer, si l'écran d'accueil du programme d'installation ne s'affiche pas, réinitialisez les paramètres par défaut du terminal.
2. Appuyez sept fois sur l'écran du terminal.
Un lecteur de QR Code s'ouvre sur le terminal.
3. Scannez le QR Code qui vous a été fourni par votre administrateur.
4. Spécifiez les informations de connexion à votre réseau Wi-Fi professionnel, y compris l'**adresse Web PAC** fournie par votre administrateur.
L'appareil installe BlackBerry UEM Client et lance le processus d'activation. Le processus d'activation prend plusieurs minutes.
5. Répondez à toutes les invites sur le terminal, y compris en fournissant le mot de passe d'activation le cas échéant, en acceptant les contrats de licence, en configurant un profil professionnel et en créant un mot de passe de terminal.
6. Si nécessaire, selon la configuration de votre serveur, lorsque l'activation s'interrompt, connectez le terminal à un ordinateur de votre réseau à l'aide d'un câble USB-C avant de continuer.

À la fin : Pour vérifier que le processus d'activation a réussi, effectuez l'une des actions suivantes :

- Sur le terminal, ouvrez UEM Client. Sélectionnez **À propos de**. Dans la section **Terminal activé**, assurez-vous de la présence des informations sur le terminal et de l'heure et de la date d'activation.
- Dans BlackBerry UEM Self-Service, vérifiez que votre terminal est répertorié en tant que terminal activé. Le statut peut prendre jusqu'à deux minutes pour se mettre à jour après que vous avez activé le terminal.

Activer un terminal Samsung Knox Workspace

Ces instructions s'appliquent également aux activations Android Enterprise (Travail et Personnel - Confidentialité des données de l'utilisateur). Envoyez les instructions d'activation suivantes à l'utilisateur du terminal.

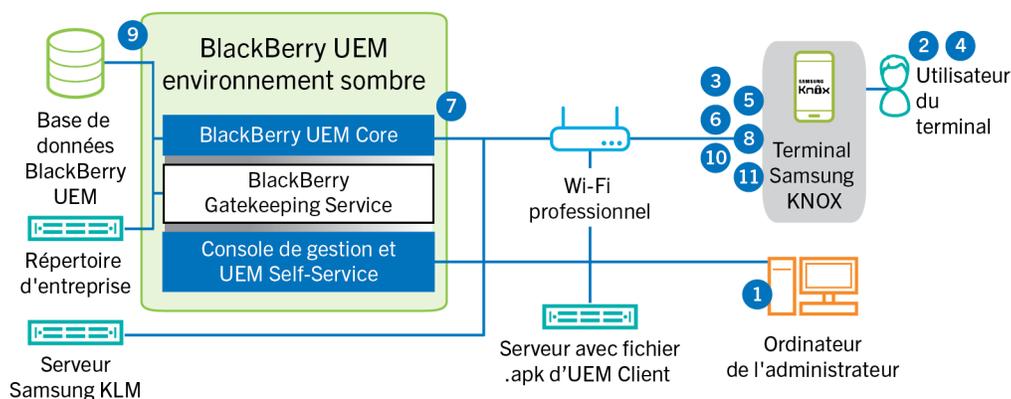
1. Connectez le terminal au réseau Wi-Fi professionnel.
2. Téléchargez et installez BlackBerry UEM Client à partir de l'emplacement fourni par votre administrateur.
3. Sur le terminal, sélectionnez **UEM Client**.
4. Lisez le contrat de licence. Sélectionnez **J'accepte**.
5. Saisissez votre adresse électronique professionnelle. Appuyez sur **Suivant**.

6. Saisissez l'adresse du serveur. Appuyez sur **Suivant**. Vous trouverez l'adresse du serveur dans l'e-mail d'activation que vous avez reçu ou dans BlackBerry UEM Self-Service.
7. Saisissez votre mot de passe d'activation. Appuyez sur **Activer mon terminal**.
8. Appuyez sur **Suivant**.
9. Appuyez sur **Activer**.

À la fin : Pour vérifier que le processus d'activation a réussi, effectuez l'une des actions suivantes :

- Sur le terminal, ouvrez UEM Client. Sélectionnez **À propos de**. Dans la section **Terminal activé**, assurez-vous de la présence des informations sur le terminal et de l'heure et de la date d'activation.
- Dans BlackBerry UEM Self-Service, vérifiez que votre terminal est répertorié en tant que terminal activé. Le statut peut prendre jusqu'à deux minutes pour se mettre à jour après que vous avez activé le terminal.

Flux de données : Activation d'un terminal Android Enterprise

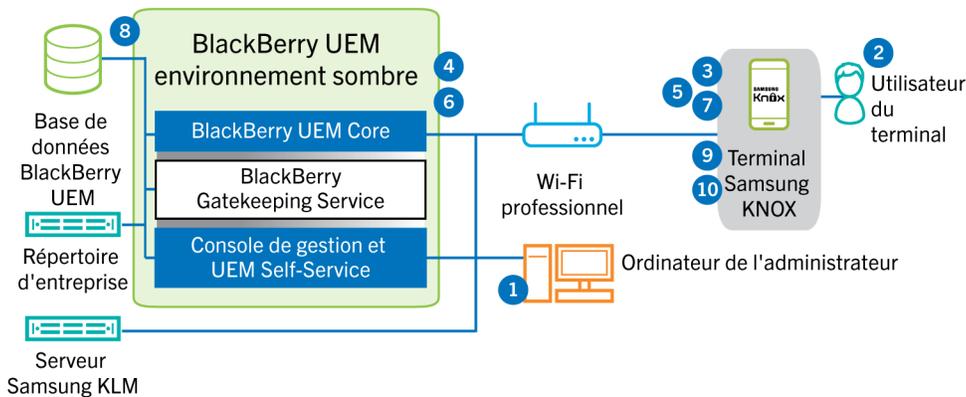


Ce flux de données s'applique aux terminaux activés avec les types d'activation Android Enterprise (Espace Travail uniquement) ou (Travail et Personnel - Contrôle total).

1. Vous effectuez les opérations suivantes :
 - a. Ajouter un utilisateur à BlackBerry UEM en tant que compte d'utilisateur local ou à l'aide des informations de compte récupérées depuis votre répertoire d'entreprise
 - b. Garantir que le type d'activation Android Enterprise (Espace Travail uniquement) ou Travail et Personnel - Contrôle total est attribué à l'utilisateur
 - c. Autorisez les QR Codes d'activation pour inclure le mot de passe d'activation et l'emplacement de téléchargement de BlackBerry UEM Client.
2. L'utilisateur réinitialise les paramètres par défaut de son terminal.
3. Le terminal redémarre et affiche un écran de bienvenue ou de démarrage.
4. L'utilisateur effectue les opérations suivantes :
 - a. Il ouvre l'e-mail d'activation reçu sur son ordinateur ou un autre appareil
 - b. Il appuie sept fois sur l'écran du terminal pour ouvrir un lecteur de QR Codes
 - c. Il connecte le terminal au réseau Wi-Fi professionnel.
 - d. Il scanne le QR Code dans l'email d'activation
5. Le terminal effectue les opérations suivantes :
 - a. Il invite l'utilisateur à crypter le terminal et redémarre.
 - b. Il télécharge le UEM Client à partir de l'emplacement de téléchargement spécifié par le QR Code et l'installe
6. Le UEM Client établit une connexion avec BlackBerry UEM et envoie une demande d'activation à BlackBerry UEM. La demande d'activation comprend le nom d'utilisateur, le mot de passe, le système d'exploitation du terminal et un identifiant de terminal unique.

7. BlackBerry UEM effectue les opérations suivantes :
 - a. Il vérifie que les informations d'identification sont valides.
 - b. Il crée une instance de terminal.
 - c. Il associe l'instance de terminal au compte d'utilisateur spécifié dans la base de données BlackBerry UEM
 - d. Il ajoute l'ID de la session d'inscription à une session HTTP
 - e. Il envoie un message d'authentification réussie au terminal
8. Le UEM Client demande toutes les informations de configuration et envoie les informations relatives au terminal et au logiciel à BlackBerry UEM.
9. BlackBerry UEM stocke les informations relatives au terminal dans la base de données et envoie les informations de configuration demandées au terminal.
10. UEM Client détermine si le terminal utilise Knox Platform for Enterprise et exécute une version prise en charge. Si le terminal utilise Knox Platform for Enterprise, le terminal se connecte au serveur KLM Samsung local et active la licence de gestion Knox. Une fois celle-ci activée, UEM Client applique les règles de stratégie informatique Android Enterprise appropriées.
11. Le terminal envoie un accusé de réception à BlackBerry UEM pour lui confirmer qu'il a reçu et appliqué les informations de configuration. Le processus d'activation est terminé.

Flux de données : Activation d'un terminal pour utiliser Knox Workspace



1. Vous effectuez les opérations suivantes :
 - a. Ajoutez un utilisateur à BlackBerry UEM en tant que compte d'utilisateur local ou à l'aide des informations de compte récupérées depuis votre répertoire d'entreprise.
 - b. Assurez-vous que le type d'activation « Travail et Personnel - Contrôle total (Samsung Knox) » ou « Espace Travail uniquement (Samsung Knox) » est attribué à l'utilisateur.
 - c. Dites à l'utilisateur de télécharger et installer le BlackBerry UEM Client :
 - d. Utilisez l'une des options suivantes pour fournir les détails d'activation à l'utilisateur :
 - Générez automatiquement un mot de passe d'activation du terminal et envoyez un e-mail contenant les instructions d'activation à l'utilisateur
 - Définissez un mot de passe d'activation du terminal et communiquez le nom d'utilisateur et le mot de passe à l'utilisateur directement ou par e-mail.
 - Communiquez l'adresse de BlackBerry UEM Self-Service à l'utilisateur afin qu'il puisse définir son propre mot de passe d'activation
2. L'utilisateur effectue les opérations suivantes :
 - Il se connecte à votre réseau Wi-Fi professionnel
 - Il télécharge et installe le UEM Client sur le terminal
 - Il ouvre le UEM Client et saisit l'adresse électronique et le mot de passe d'activation

3. Le UEM Client établit une connexion avec BlackBerry UEM et envoie une demande d'activation à BlackBerry UEM. La demande d'activation comprend le nom d'utilisateur, le mot de passe, le système d'exploitation du terminal et un identifiant de terminal unique.
4. BlackBerry UEM effectue les opérations suivantes :
 - a. Il vérifie que les informations d'identification sont valides.
 - b. Il crée une instance de terminal.
 - c. Il associe l'instance de terminal au compte d'utilisateur spécifié dans la base de données BlackBerry UEM.
 - d. Il ajoute l'ID de la session d'inscription à une session HTTP.
 - e. Il envoie un message d'authentification réussie au terminal.
5. Le UEM Client crée un CSR à l'aide des informations reçues de BlackBerry UEM et envoie une demande de certificat client à BlackBerry UEM via HTTPS.
6. BlackBerry UEM effectue les actions suivantes :
 - a. Il valide la demande de certificat client en la comparant à l'ID de session d'inscription dans la session HTTP.
 - b. Il signe la demande de certificat client avec le certificat racine.
 - c. Il renvoie le certificat client signé et le certificat racine à UEM Client.

Une session TLS avec authentification mutuelle est établie entre le UEM Client et BlackBerry UEM.

7. Le UEM Client demande toutes les informations de configuration et envoie les informations relatives au terminal et au logiciel à BlackBerry UEM.
8. BlackBerry UEM stocke les informations relatives au terminal dans la base de données et envoie les informations de configuration demandées au terminal.
9. Le UEM Client détermine si le terminal utilise Knox Workspace et exécute une version prise en charge. Si le terminal utilise Knox Workspace, le terminal se connecte au serveur KLM Samsung local et active la licence de gestion Knox. Une fois celle-ci activée, le UEM Client applique les règles de stratégie informatique Knox MDM et Knox Workspace.
10. Le terminal envoie un accusé de réception à BlackBerry UEM pour lui confirmer qu'il a reçu et appliqué les informations de configuration. Le processus d'activation est terminé.

Au terme de l'activation, l'utilisateur est invité à créer un mot de passe d'espace Travail pour Knox Workspace. Les données de Knox Workspace sont protégées à l'aide du cryptage et d'une méthode d'authentification, comme un mot de passe, un PIN, un motif ou une empreinte digitale.

Remarque : Si le terminal est activé avec le type d'activation « Espace Travail uniquement - (Samsung Knox) », l'espace Personnel est supprimé lorsque Knox Workspace est configuré.

Activation des terminaux iOS

Si vous autorisez les utilisateurs à utiliser des terminaux iOS dans un environnement de site sombre, vous devez préparer les terminaux à l'aide de Apple Configurator 2. BlackBerry UEM ne prend pas en charge les terminaux inscrits dans le programme d'inscription de terminaux de Apple. Les utilisateurs terminent l'activation pour les terminaux préparés sans utiliser l'application BlackBerry UEM Client. Ils ont uniquement besoin de leur nom d'utilisateur et du mot de passe d'activation.

Une fois les terminaux activés, BlackBerry UEM leur transmet la stratégie informatique et les profils que vous avez attribués aux utilisateurs.

Étapes à suivre pour activer des terminaux iOS

Étape	Action
1	Ajouter les informations relatives au serveur BlackBerry UEM dans Apple Configurator 2.
2	Préparer les terminaux iOS à l'aide de Apple Configurator 2.
3	Créez un profil d'activation et attribuez-le à un compte d'utilisateur ou à un groupe d'utilisateurs.
4	Définir un mot de passe d'activation et envoyer un e-mail d'activation.
5	Distribuez les terminaux aux utilisateurs et demandez-leur de terminer la configuration.

Ajouter les informations relatives au serveur BlackBerry UEM dans Apple Configurator 2

Avant de commencer : Téléchargez et installez la dernière version de Apple Configurator 2 à partir de Apple.

1. Dans le menu de Apple Configurator 2, sélectionnez **Préférences > Serveurs**.
2. Cliquez sur **+** > **Suivant**.
3. Dans le champ **Nom**, saisissez un nom pour le serveur.
4. Dans le champ **Nom d'hôte ou URL**, saisissez l'URL du serveur BlackBerry UEM au format suivant : *<http ou https>://<nom_serveur>:<port>*, sachant que le numéro de port par défaut est 8885. Pour plus d'informations sur les paramètres de port, [reportez-vous à la section BlackBerry UEM Ports d'écoute](#) du contenu relatif à la planification.
5. Cliquez sur **Suivant**.
6. Fermez la fenêtre **Serveur**.

Préparer les terminaux iOS à l'aide de Apple Configurator 2

Lorsque vous préparez un terminal, Apple Configurator 2 le nettoie et procède à une mise à niveau du système d'exploitation vers la version la plus récente.

Avant de commencer : [Ajouter les informations relatives au serveur BlackBerry UEM dans Apple Configurator 2](#).

1. Ouvrez Apple Configurator 2.
2. Connectez un ou plusieurs terminaux iOS à votre ordinateur.
3. Cliquez sur **Préparer**.
4. Dans la liste déroulante **Configuration**, sélectionnez **Manuelle**. Cliquez sur **Suivant**.
5. Dans la liste déroulante **Serveur**, sélectionnez le serveur BlackBerry UEM. Cliquez sur **Suivant**.
6. Vous pouvez également cocher la case **Superviser les terminaux**. Cliquez sur **Suivant**.
7. Si vous avez sélectionné **Superviser les terminaux**, entrez les informations relatives à l'entreprise.
8. Cliquez sur **Préparer** et attendez que le terminal soit prêt. Le processus peut prendre une quinzaine de minutes.

À la fin : Distribuez les terminaux aux utilisateurs pour qu'ils puissent terminer l'activation.

Gestion des terminaux BlackBerry 10

Pour plus de détails sur la gestion des terminaux BlackBerry 10 et des utilisateurs de terminaux, reportez-vous au [contenu relatif à l'administration de BlackBerry UEM](#).

Vous devriez garder les considérations suivantes à l'esprit lors de la gestion de terminaux BlackBerry 10 dans un environnement de site sombre.

Considérations relatives aux sites sombres	Description
Connexion aux ressources de votre organisation	Dans un environnement de site sombre, les terminaux BlackBerry 10 peuvent se connecter à votre réseau en utilisant uniquement votre réseau Wi-Fi professionnel ou un VPN. Pour utiliser un VPN, assurez-vous d'installer une application VPN appropriée sur le terminal et de définir un profil VPN.
Gestion des applications	BlackBerry UEM pour les sites sombres ne prend pas en charge les connexions à BlackBerry World. Vous ne pouvez pas ajouter d'applications publiques à la liste des applications pour les terminaux.

Gestion des terminaux Samsung Knox

Pour plus de détails sur la gestion des terminaux Samsung Knox et des utilisateurs de terminaux, [reportez-vous au contenu relatif à l'administration de BlackBerry UEM](#).

Vous devriez garder les considérations suivantes à l'esprit lors de la gestion de terminaux Samsung Knox dans un environnement de site sombre.

Considérations relatives aux sites sombres	Description
Connexion aux ressources de votre organisation	Dans un environnement de site sombre, après activation, les terminaux Samsung Knox peuvent se connecter à BlackBerry UEM et à vos ressources à l'aide d'une connexion VPN. Pour plus d'informations, reportez-vous à Configurer le VPN à l'aide de KNOX StrongSwan .
Gestion des applications	BlackBerry UEM pour les sites sombres ne prend pas en charge les connexions à Google Play. Vous ne pouvez pas ajouter d'applications publiques à la liste des applications pour les terminaux.
Données d'e-mail et d'organiseur	L'application de messagerie par défaut sur les terminaux Samsung Knox a besoin de se connecter à l'infrastructure Samsung avant d'envoyer et de recevoir des données. Vous pouvez choisir d'autoriser cette connexion ou d'utiliser une autre application de messagerie sur les terminaux Samsung Knox.

Considérations relatives aux sites sombres	Description
Notifications de terminal	L'envoi de notifications aux terminaux Samsung Knox à l'aide de GCM n'est pas pris en charge dans un environnement de site sombre. Le BlackBerry UEM Client sondera BlackBerry UEM en quête de mises à jour à intervalles réguliers.

Configurer le VPN à l'aide de KNOX StrongSwan

Vous pouvez configurer un accès VPN à votre environnement pour les terminaux Samsung Knox.

Avant de commencer : Téléchargez les applications Knox Service Plugin et Android VPN Management for KNOX StrongSwan, et ajoutez les fichiers .apk à l'[emplacement réseau partagé des applications internes](#).

1. Ajoutez les applications Knox Service Plugin et Android VPN Management for KNOX StrongSwan à la [liste des applications](#).
2. Sélectionnez l'application Knox Service Plugin et cliquez sur  pour définir [les options de configuration de l'application](#).
 - a) Sous **Profil VPN**, sélectionnez **VPN intégré KNOX**.
 - b) Sous **Paramètres du VPN intégré KNOX (pour StrongSwan)**, définissez les options suivantes :
 - Définissez le **type d'authentification** sur « ipsec_ike2_rsa ».
 - Définissez l'**alias du certificat utilisateur** sur le nom d'utilisateur auquel est ajouté « _1 [Knox] ». Vous pouvez utiliser [des variables](#) pour le nom d'utilisateur (par exemple %UserFirstName % %UserLastName% _1 [KNOX].)
 - Définissez l'**alias du certificat d'autorité de certification** sur le nom d'utilisateur auquel est ajouté « [Knox] ». Vous pouvez utiliser [des variables](#) pour le nom d'utilisateur (par exemple %UserFirstName % %UserLastName% [KNOX].)
3. Attribuez l'application à l'utilisateur.
4. [Créez un profil de certificat d'autorité de certification partagé](#) pour envoyer le certificat de serveur VPN aux terminaux et l'attribuer aux utilisateurs.
5. [Ajoutez un certificat client VPN](#) pour chaque utilisateur.

Gestion des terminaux iOS

Pour plus de détails sur la gestion des terminaux iOS et des utilisateurs de terminaux, [reportez-vous au contenu relatif à l'administration de BlackBerry UEM](#).

Vous devriez garder les considérations suivantes à l'esprit lors de la gestion de terminaux iOS dans un environnement de site sombre.

Considérations relatives aux sites sombres	Description
Connexion aux ressources de votre organisation	Dans un environnement de site sombre, après activation, les terminaux iOS peuvent se connecter à BlackBerry UEM et à vos ressources à l'aide d'une connexion VPN. Pour utiliser un VPN, assurez-vous d'installer une application VPN appropriée sur le terminal et de définir un profil VPN.

Considérations relatives aux sites sombres	Description
Gestion des applications	BlackBerry UEM pour les sites sombres ne prend pas en charge les connexions à Apple App Store. Vous ne pouvez pas ajouter d'applications publiques à la liste des applications pour les terminaux.
Profils de conformité	Parce que le client BlackBerry UEM Client n'est pas pris en charge pour les terminaux iOS dans un environnement de site sombre, les profils de conformité ne sont pas pris en charge.

Documentation produit

Le contenu BlackBerry UEM suivant devrait vous être utile lors de la gestion de BlackBerry UEM dans un environnement de site sombre.

Si vos exigences en matière de sécurité de sites sombres vous empêchent d'accéder à la documentation BlackBerry UEM depuis la console de gestion, vous pouvez télécharger les versions PDF de la documentation depuis un emplacement doté d'un accès complet à Internet ou demander à votre représentant de l'assistance client BlackBerry de vous les envoyer.

Ressource	Description
Notes de version	<ul style="list-style-type: none">• Descriptions des problèmes résolus• Description des problèmes connus et des éventuelles solutions de contournement• Nouveautés
Installation et mise à niveau	<ul style="list-style-type: none">• Configuration système requise• Instructions d'installation• Instructions de mise à niveau
Configuration	<ul style="list-style-type: none">• Instructions sur la configuration des composants de serveur avant de commencer à administrer les utilisateurs et leurs terminaux• Instructions sur la migration des données depuis une base de données BlackBerry UEM existante
Administration	<ul style="list-style-type: none">• Administration basique et avancée pour tous les types de terminaux pris en charge• Instructions sur la création de comptes, groupes, rôles d'utilisateur et comptes d'administrateurs• Instructions d'activation de terminaux• Instructions de création et d'envoi de stratégies informatiques et de profils• Instructions de gestion des applications sur les terminaux• Descriptions des paramètres de profil• Descriptions des règles de stratégie informatique pour les terminaux BlackBerry 10, iOS et Android
Matrice de compatibilité	<ul style="list-style-type: none">• Liste des systèmes d'exploitation, serveurs de base de données et navigateurs pris en charge par le serveur BlackBerry UEM• Liste des systèmes d'exploitation de terminal pris en charge

Informations juridiques

©2022 BlackBerry Limited. Les marques commerciales, notamment BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE et SECUSMART sont des marques commerciales ou des marques déposées de BlackBerry Limited, ses filiales et/ou sociétés affiliées, utilisées sous licence, et les droits exclusifs de ces marques commerciales sont expressément réservés. Toutes les autres marques commerciales appartiennent à leurs propriétaires respectifs.

Cette documentation, y compris la documentation incluse pour référence telle que celle fournie ou mise à disposition sur le site Web BlackBerry, est fournie ou mise à disposition « EN L'ÉTAT » et « TELLE QUELLE », sans condition ni garantie en tout genre de la part de BlackBerry Limited et de ses filiales (« BlackBerry »), et BlackBerry décline toute responsabilité en cas d'erreur ou d'oubli typographique, technique ou autre inexactitude contenue dans ce document. Pour des raisons de protection des informations confidentielles et/ou des secrets commerciaux de BlackBerry, cette documentation peut décrire certains aspects de la technologie BlackBerry en termes généraux. BlackBerry se réserve le droit de modifier périodiquement les informations contenues dans cette documentation. Cependant, BlackBerry ne s'engage en aucune manière à vous communiquer les modifications, mises à jour, améliorations ou autres ajouts apportés à cette documentation.

La présente documentation peut contenir des références à des sources d'informations, du matériel ou des logiciels, des produits ou des services tiers, y compris des composants et du contenu tel que du contenu protégé par copyright et/ou des sites Web tiers (ci-après dénommés collectivement « Produits et Services tiers »). BlackBerry ne contrôle pas et décline toute responsabilité concernant les Produits et Services tiers, y compris, sans s'y limiter, le contenu, la précision, le respect du code de la propriété intellectuelle, la compatibilité, les performances, la fiabilité, la légalité, l'éthique, les liens ou tout autre aspect desdits Produits et Services tiers. La présence d'une référence aux Produits et Services tiers dans cette documentation ne suppose aucunement que BlackBerry se porte garant des Produits et Services tiers ou de la tierce partie concernée.

SAUF DANS LA MESURE SPÉCIFIQUEMENT INTERDITE PAR LES LOIS EN VIGUEUR DANS VOTRE JURIDICTION, TOUTES LES CONDITIONS, GARANTIES OU REPRÉSENTATIONS DE TOUTE NATURE, EXPRESSES OU TACITES, NOTAMMENT (SANS LIMITATIONS) LES CONDITIONS, GARANTIES OU REPRÉSENTATIONS DE DURABILITÉ, D'ADÉQUATION À UNE UTILISATION OU À UN BUT PARTICULIER, DE COMMERCIALISATION, DE QUALITÉ MARCHANDE, DE NON-INFRACTION, DE SATISFACTION DE LA QUALITÉ OU DE TITRE, OU RÉSULTANT D'UNE LOI, D'UNE COUTUME, D'UNE PRATIQUE OU D'UN USAGE COMMERCIAL, OU EN RELATION AVEC LA DOCUMENTATION OU SON UTILISATION, OU LA PERFORMANCE OU NON-PERFORMANCE DES LOGICIELS, DU MATÉRIEL, DES SERVICE OU DES PRODUITS ET SERVICES TIERS CITÉS, SONT EXCLUES. VOUS POUVEZ JOUIR D'AUTRES DROITS QUI VARIENT SELON L'ÉTAT OU LA PROVINCE. CERTAINES JURIDICTIONS N'AUTORISENT PAS L'EXCLUSION OU LA LIMITATION DES GARANTIES ET CONDITIONS IMPLICITES. DANS LA MESURE AUTORISÉE PAR LES LOIS, TOUTE GARANTIE OU CONDITION IMPLICITE RELATIVE À LA DOCUMENTATION, DANS LA MESURE OÙ ELLES NE PEUVENT PAS ÊTRE EXCLUES EN VERTU DES CLAUSES PRÉCÉDENTES, MAIS PEUVENT ÊTRE LIMITÉES, SONT PAR LES PRÉSENTES LIMITÉES À QUATRE-VINGT-DIX (90) JOURS À COMPTER DE LA DATE DE LA PREMIÈRE ACQUISITION DE LA DOCUMENTATION OU DE L'ARTICLE QUI FAIT L'OBJET D'UNE RÉCLAMATION.

DANS LA MESURE MAXIMALE PERMISE PAR LES LOIS EN VIGUEUR DANS VOTRE JURIDICTION, EN AUCUN CAS BLACKBERRY N'EST RESPONSABLE DES DOMMAGES LIÉS À LA PRÉSENTE DOCUMENTATION OU À SON UTILISATION, OU À LA PERFORMANCE OU NON-PERFORMANCE DES LOGICIELS, DU MATÉRIEL, DES SERVICES OU DES PRODUITS ET SERVICES TIERS MENTIONNÉS DANS LES PRÉSENTES, ET NOTAMMENT, SANS S'Y LIMITER, DES DOMMAGES DIRECTS, EXEMPLAIRES, ACCIDENTELS, INDIRECTS, SPÉCIAUX, PUNITIFS OU AGGRAVÉS, DES DOMMAGES LIÉS À UNE PERTE DE PROFITS OU DE REVENUS, UN MANQUE À GAGNER, UNE INTERRUPTION D'ACTIVITÉ, UNE PERTE D'INFORMATIONS COMMERCIALES, UNE PERTE D'OPPORTUNITÉS COMMERCIALES, LA CORRUPTION OU LA PERTE DE DONNÉES, LE NON-ENVOI OU LA NON-RÉCEPTION DE DONNÉES, DES PROBLÈMES LIÉS À DES APPLICATIONS UTILISÉES AVEC DES PRODUITS OU SERVICES BLACKBERRY, DES COÛTS D'INDISPONIBILITÉ, LA PERTE D'UTILISATION DES PRODUITS OU SERVICES BLACKBERRY EN TOUT OU EN PARTIE, OU DE TOUT SERVICE DE COMMUNICATION, DU COÛT DE BIENS DE

SUBSTITUTION, DES FRAIS DE GARANTIE, DES ÉQUIPEMENTS OU SERVICES, DES COÛTS DE CAPITAL, OU AUTRES PERTES FINANCIÈRES SIMILAIRES, PRÉVISIBLES OU NON, MÊME SI BLACKBERRY A ÉTÉ INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES.

DANS LA MESURE MAXIMALE PERMISE PAR LES LOIS APPLICABLES DANS VOTRE JURIDICTION, BLACKBERRY N'EST NULLEMENT TENU PAR DES OBLIGATIONS, DEVOIRS OU RESPONSABILITÉS, CONTRACTUELS, DÉLICTELS OU AUTRES, PAS MÊME PAR UNE RESPONSABILITÉ EN CAS DE NÉGLIGENCE OU RESPONSABILITÉ STRICTE ET NE VOUS EST REDEVABLE EN RIEN.

LES LIMITATIONS, EXCLUSIONS ET CLAUSES DE NON-RESPONSABILITÉ CONTENUES DANS LES PRÉSENTES S'APPLIQUENT : (A) INDÉPENDAMMENT DE LA NATURE DE LA CAUSE D'ACTION, DE DEMANDE OU D'ACTION ENTREPRISE PAR VOUS, NOTAMMENT, SANS S'Y LIMITER, POUR RUPTURE DE CONTRAT, NÉGLIGENCE, FAUTE, RESPONSABILITÉ STRICTE OU TOUTE AUTRE THÉORIE LÉGALE, ET RESTENT APPLICABLES EN CAS DE RUPTURES SUBSTANTIELLES OU DE MANQUEMENT AU BUT ESSENTIEL DU PRÉSENT CONTRAT OU DE TOUT RECOURS ENVISAGEABLE PAR LES PRÉSENTES ; ET (B) À BLACKBERRY ET À SES FILIALES, LEURS AYANTS DROIT, REPRÉSENTANTS, AGENTS, FOURNISSEURS (NOTAMMENT LES FOURNISSEURS DE SERVICES), REVENDEURS AGRÉÉS BLACKBERRY (NOTAMMENT LES FOURNISSEURS DE SERVICES) ET LEURS DIRECTEURS, EMPLOYÉS ET SOUS-TRAITANTS RESPECTIFS.

OUTRE LES LIMITATIONS ET EXCLUSIONS SUSMENTIONNÉES, EN AUCUN CAS, LES DIRECTEURS, EMPLOYÉS, AGENTS, REVENDEURS, FOURNISSEURS, SOUS-TRAITANTS DE BLACKBERRY OU DE SES FILIALES N'ONT UNE RESPONSABILITÉ CONSÉCUTIVE OU RELATIVE À LA PRÉSENTE DOCUMENTATION.

Avant de vous abonner, d'installer ou d'utiliser des Produits et Services tiers, il est de votre responsabilité de vérifier que votre fournisseur de services prend en charge toutes les fonctionnalités. Certains fournisseurs de services peuvent ne pas proposer de fonctionnalités de navigation Internet avec un abonnement à BlackBerry® Internet Service. Vérifiez auprès de votre fournisseur de services la disponibilité, les accords d'itinérance, les plans de service et les fonctionnalités. L'installation ou l'utilisation de Produits et Services tiers avec des produits et services BlackBerry peuvent nécessiter un ou plusieurs brevets, marques commerciales, licences de copyright ou autres licences à des fins de protection des droits d'autrui. Vous êtes seul responsable de votre décision d'utiliser ou non les Produits et Services tiers et si cela nécessite l'obtention de licences tierces. Si de telles licences sont requises, vous êtes seul responsable de leur acquisition. Vous ne devez pas installer ou utiliser de Produits et Services tiers avant d'avoir acquis la totalité des licences nécessaires. Les Produits et Services tiers fournis avec les produits et services BlackBerry vous sont fournis à toutes fins utiles « EN L'ÉTAT » sans conditions, garanties ou représentations expresses ou tacites d'aucune sorte par BlackBerry, et BlackBerry n'engage aucune responsabilité sur les Produits et Services tiers à cet égard. L'utilisation que vous faites des Produits et Services tiers est régie par et dépendante de votre acceptation des termes des licences et autres accords distincts applicables à cet égard avec d'autres parties, sauf dans la limite couverte expressément par une licence ou autre accord conclu avec BlackBerry.

Les conditions d'utilisation de tout produit ou service BlackBerry sont stipulées dans une licence ou autre accord distinct conclu avec BlackBerry à cet égard. LE CONTENU DE CETTE DOCUMENTATION N'EST PAS DESTINÉ À REMPLACER LES ACCORDS OU GARANTIES EXPRÈS ET ÉCRITS FOURNIS PAR BLACKBERRY POUR UNE PARTIE DES PRODUITS OU SERVICES BLACKBERRY AUTRES QUE CETTE DOCUMENTATION.

BlackBerry Enterprise Software incorpore des éléments logiciels tiers. La licence et les informations de copyright associées à ce logiciel sont disponibles à l'adresse <http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp>.

BlackBerry Limited
2200 University Avenue Est
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,

Maidenhead, Berkshire SL6 1RL
Royaume-Uni

Publié au Canada